

Injectivity of Compressing Maps on the Set of Primitive Sequences over $\mathbb{Z}/p^e\mathbb{Z}$

Lin Wang¹ *and Zhi Hu²

1. *Science and Technology on Communication Security Laboratory*

Chengdu, 610041, P. R. China

e-mail:lin.wang4math@gmail.com

2. *Beijing International Center for Mathematical Research, Peking University*

Beijing, 100871, P. R. China

e-mail:huzhi@math.pku.edu.cn

Abstract

Let $\sigma(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/p^e\mathbb{Z}$ with p a prime, and let G be the set of primitive linear recurring sequences generated by $\sigma(x)$. A map f on $\mathbb{Z}/p^e\mathbb{Z}$ naturally induces a map \hat{f} on G , mapping a sequence $(\dots, s_{i-1}, s_i, s_{i+1}, \dots)$ to $(\dots, f(s_{i-1}), f(s_i), f(s_{i+1}), \dots)$. Whether the induced map \hat{f} is injective on G is studied. If $p \geq 3$ and $(x^{(p^n-1)} - 1)^2/p^2 \not\equiv a \pmod{(p, \sigma(x))}$ for any $a \in \mathbb{F}_p$, then \hat{f} is injective if and only if for any m -th root of unity γ , where m is a prime divisor of $p-1$, there exists $a \in \mathbb{Z}/p^e\mathbb{Z}$ such that f is not constant on $\{\gamma^i a : 1 \leq i \leq m\}$. Furthermore, conventionally $a \in \mathbb{Z}/p^e\mathbb{Z}$ is identified with the vector $(a_0, a_1, \dots, a_{e-1}) \in \mathbb{F}_p^e$, where $a = a_0 + a_1p + \dots + a_{e-1}p^{e-1}$ and $a_i \in \{0, 1, \dots, p-1\}$. Then for $p \geq 3$ three kinds of maps below induce injective maps on G :

$$f(x_0, \dots, x_{e-1}) = x_{e-1}^\ell f_1(x_0, x_1, \dots, x_{e-2}) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $2 \leq \ell < p$, $(x_0^{p-1} - 1) \nmid f_1$ and $x_0 \nmid f_1$;

$$f(x_0, \dots, x_{e-1}) = x_{e-1}(g_0(x_k) + g_1(x_0, x_1, \dots, x_{k-1})) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $\deg g_0 \geq 1$ if $1 \leq k \leq e-2$, $x_0 \nmid g_0$ if $k=0$, and $\gcd(p-1, \deg g_0 + 1) = 1$;

$$f(x_0, \dots, x_{e-1}) = f_0(x_{e-1})f_1(x_0, x_1, \dots, x_{e-2}) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $1 \leq \deg f_0 < p$, $(x_0^{p-1} - 1) \nmid f_1$, $f_1(0, 0, \dots, 0) \neq 0$ and $\sigma(x)$ is strongly primitive.

Key Words: residue class ring, p -adic ring, compressing map, primitive sequence, equivalence closure.

1 Introduction

Pseudorandom sequences play a significant role in coding, cryptography and communication systems. A kind of candidates are compressed sequences derived from a linear feedback shift

*This work was supported by the Applied Basic Research Program of the Sichuan Province, P. R. China (Grant No. 2011JY0143).

register(abbr. LFSR) over the residue class ring $\mathbb{Z}/p^e\mathbb{Z}$, where p is a prime [7, 9–12, 14, 15, 25, 26]. As in Fig.1, such a sequence generator consists of a compressing map f defined on $\mathbb{Z}/p^e\mathbb{Z}$ and an

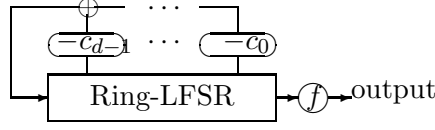


Figure 1: A PRNG by ring-LFSR

LFSR abiding by a linear recurring relation $\vec{s}(i) = -c_{n-1}\vec{s}(i-1) - \dots - c_0\vec{s}(i-n)$ over $\mathbb{Z}/p^e\mathbb{Z}$. The LFSR in Fig.1 has its characteristic polynomial

$$\sigma(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0, c_i \in \mathbb{Z}/p^e\mathbb{Z}. \quad (1)$$

If $\min\{0 < m \in \mathbb{Z} : \sigma(x) \mid x^m - 1\} = p^{e-1}(p^n - 1)$, then $\sigma(x)$ is said to be *primitive*. Unless $e = p = 2$ let $h(x)$ be the polynomial over \mathbb{F}_p satisfying $h(x) \equiv (x^{p(p^n-1)} - 1)/p^2 \pmod{(p, \sigma(x))}$. If $\sigma(x)$ is primitive and additionally $\deg h(x) \geq 1$, then $\sigma(x)$ is said to be *strongly primitive*.

The compressing map f in Fig.1 naturally induces a map \hat{f} on the set of primitive sequences generated by $\sigma(x)$. Specifically, a sequence $(\dots, s_{i-1}, s_i, s_{i+1}, \dots)$ is mapped to $(\dots, f(s_{i-1}), f(s_i), f(s_{i+1}), \dots)$. If the induced map \hat{f} is injective, f is called *entropy-preserving* [15, 23]. Entropy preservation of compressing maps has hitherto attracted extensive study [7, 8, 15, 16, 19, 23, 24, 26, 30, 34, 35]. Given an odd prime p , for an integer M which is not a power of p and two primitive sequences \vec{a} and \vec{b} outputted from the same generator, [35] proved that $\vec{a} \equiv \vec{b} \pmod{M}$ if and only if $\vec{a} = \vec{b}$. Since $a \in \mathbb{Z}/p^e\mathbb{Z}$ has a unique representative written as $a = a_0 + a_1p + \dots + a_{e-1}p^{e-1}$, $a_i \in \{0, 1, \dots, p-1\}$, in [7, 8, 15, 16, 23, 24, 26, 30, 34, 35] a function $\mathbb{Z}/p^e\mathbb{Z} \rightarrow \mathbb{F}_p$ is naturally interpreted as an e -variable polynomial over \mathbb{F}_p , and a sequence \vec{s} over $\mathbb{Z}/p^e\mathbb{Z}$ is written uniquely as $\vec{s} = \vec{s}_0 + \vec{s}_1p + \dots + \vec{s}_{e-1}p^{e-1}$, where \vec{s}_i is a sequence over $\{0, 1, \dots, p-1\}$, $i = 0, 1, \dots, e-1$. It is known by [7, 8, 12] that the *highest level sequence* \vec{s}_{e-1} of a primitive sequence \vec{s} contains the same information as \vec{s} . For $p \geq 5$ and $e \geq 2$, Zhu and Qi [30] designed a family of entropy-preserving maps

$$f(x_0, \dots, x_{e-1}) = x_{e-1}^\ell + f_2(x_0, \dots, x_{e-2}), \quad (2)$$

where $2 \leq \ell \leq p-1$. Besides, given $p \geq 3$ and $e \geq 3$, Sun and Qi [23] found a kind of entropy-preserving maps

$$f(x_0, \dots, x_{e-1}) = x_{e-1}(g_0(x_{e-2}) + g_1(x_0, x_1, \dots, x_{e-3})) + g_2(x_0, \dots, x_{e-2}), \quad (3)$$

where $\deg g_0 \geq 2$ and $\gcd(1 + \deg g_0, p-1) = 1$. Furthermore, thanks to [15–17, 24, 30, 34], provided that $\sigma(x)$ is strongly primitive, the compressing map

$$f(x_0, \dots, x_{e-1}) = g_0(x_{e-1}) + g_1(x_0, \dots, x_{e-2}), \quad (4)$$

is entropy-preserving, where $1 \leq \deg g_0 \leq p-1$. Additionally, pseudorandom properties of the highest level sequences were studied, e.g. distribution of zeros and ones [4, 6, 17, 18, 22], linear complexity [3, 9] and nonlinear complexity [32]. Moreover, [27, 31, 33, 35] gave compressing maps such that distribution of zeros in the compressed sequence implies all information of the original

primitive sequence. Recently, entropy preservation of maximal length sequences over $\mathbb{Z}/N\mathbb{Z}$, where N is an odd square-free integer, is also considered [1, 28, 29].

Our contribution. For most cases, particularly $p \geq 3$, this article concentrates on the inherent information of a map which yields the same compressed sequence from distinct primitive sequences. If p is an odd prime and $(x^{(p^n-1)} - 1)^2/p^2 \not\equiv a \pmod{(p, \sigma(x))}$ for any $a \in \mathbb{F}_p$, then a map ψ on $\mathbb{Z}/p^e\mathbb{Z}$ is entropy-preserving if and only if for any m -th root of unity γ , where m is a prime divisor of $p - 1$, there exists $a \in \mathbb{Z}/p^e\mathbb{Z}$ such that ψ is not constant on $\{\gamma^i a : 1 \leq i \leq m\}$. We also give a sufficient condition of entropy preservation, and thereby construct three families of entropy-preserving maps for $p \geq 3$ as below:

$$f(x_0, \dots, x_{e-1}) = x_{e-1}^\ell f_1(x_0, x_1, \dots, x_{e-2}) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $2 \leq \ell < p$, $(x_0^{p-1} - 1) \nmid f_1$ and $x_0 \nmid f_1$;

$$f(x_0, \dots, x_{e-1}) = x_{e-1}(g_0(x_k) + g_1(x_0, x_1, \dots, x_{k-1})) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $\deg g_0 \geq 1$ if $1 \leq k \leq e - 2$, $x_0 \nmid g_0$ if $k = 0$, and $\gcd(p - 1, \deg g_0 + 1) = 1$;

$$f(x_0, \dots, x_{e-1}) = f_0(x_{e-1})f_1(x_0, x_1, \dots, x_{e-2}) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $1 \leq \deg f_0 < p$, $(x_0^{p-1} - 1) \nmid f_1$, $f_1(0, 0, \dots, 0) \neq 0$ and $\sigma(x)$ is strongly primitive. Therefore, previous results of [23, 24, 30, 34] are improved.

The rest of this article is organized as follows: In Section 2, mathematical tools are included and primitive sequences over $\mathbb{Z}/p^e\mathbb{Z}$ are interpreted by the trace function over p -adic rings. Section 3 is main results, focusing on how a compressing map acts on distinct primitive sequences. In Section 4, new entropy-preserving maps are constructed. In the last section, we conclude by leaving two problems for future.

2 Preliminaries

In this section we prepare necessary mathematical notations, tools and models.

2.1 Trace of finite fields

Denote by \mathbb{F}_q the finite field of q elements and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Throughout let p be a prime, n a positive integer greater than one, and $q = p^n$.

The set of \mathbb{F}_p -linear functions on \mathbb{F}_q is a linear space of dimension n and can be parameterized by \mathbb{F}_q .

Lemma 1. [13, Theorem 2.24] *Denote the absolute trace function of \mathbb{F}_q over \mathbb{F}_p by tr . Then the linear transformation from \mathbb{F}_q into \mathbb{F}_p are exactly the mappings $\text{tr}(\alpha \cdot) : x \mapsto \text{tr}(\alpha x)$ for all $x \in \mathbb{F}_q$, $\alpha \in \mathbb{F}_q$. Furthermore, $\text{tr}(\alpha_1 \cdot) \neq \text{tr}(\alpha_2 \cdot)$ whenever α_1 and α_2 are distinct elements of \mathbb{F}_q .*

Lemma 2. Let $\gamma \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$. Then

$$\{\text{tr}(\gamma z) : \text{tr}(z) = a, z \in \mathbb{F}_q^*\} = \begin{cases} \{\gamma a\}, & \text{if } \gamma \in \mathbb{F}_p, \\ \mathbb{F}_p, & \text{if } \gamma \notin \mathbb{F}_p, a \neq 0, \\ \mathbb{F}_p, & \text{if } \gamma \notin \mathbb{F}_p, a = 0, n \geq 3, \\ \mathbb{F}_p^*, & \text{if } \gamma \notin \mathbb{F}_p, a = 0, n = 2. \end{cases}$$

Proof. If $\gamma \in \mathbb{F}_p$, then $\text{tr}(\gamma z) = \gamma \text{tr}(z) = \gamma a$.

In the rest of proof suppose $\gamma \in \mathbb{F}_q \setminus \mathbb{F}_p$, i.e. $\gamma^p \neq \gamma$. Choose $z_0 \in \mathbb{F}_q$ satisfying $\text{tr}(z_0) = a$, enforcing $z_0 = 0$ if $a = 0$. Denote $V = \{z \in \mathbb{F}_q^* : \text{tr}(z) = a\}$. By [13, Theorem 2.25],

$$V = \begin{cases} \{y^p - y : y \in \mathbb{F}_q \setminus \mathbb{F}_p\}, & \text{if } a = 0; \\ \{z_0 + y^p - y : y \in \mathbb{F}_q\}, & \text{if } a \neq 0. \end{cases}$$

For $z \in V$, we have

$$\begin{aligned} \text{tr}(\gamma z) &= \text{tr}(\gamma z_0) + \text{tr}(\gamma(y^p - y)) \\ &= \text{tr}(\gamma z_0) + \text{tr}((\gamma y)^p - \gamma y) - \text{tr}(y^p(\gamma^p - \gamma)) \\ &= \text{tr}(\gamma z_0) - \text{tr}(y^p(\gamma^p - \gamma)). \end{aligned}$$

Suppose $a \neq 0$. Then $\{\text{tr}(\gamma z) : z \in V\} = \mathbb{F}_p$ since

$$\{\text{tr}(y^p(\gamma^p - \gamma)) : y \in \mathbb{F}_q\} = \{\text{tr}(y) : y \in \mathbb{F}_q\} = \mathbb{F}_p.$$

Suppose $a = 0$. Denote $T = \{\text{tr}(y^p(\gamma^p - \gamma)) : y \in \mathbb{F}_q \setminus \mathbb{F}_p\}$. Since $\text{tr}(y^p(\gamma^p - \gamma)) = 0$ for any $y \in \mathbb{F}_p$, we have $\mathbb{F}_p^* \subset T$ and conclude that $0 \in T$ if and only if $p < q/p = |\{y \in \mathbb{F}_q : \text{tr}(y) = 0\}|$, i.e. $n > 2$. \square

2.2 Sequences and equivalence relations

In this subsection terms of binary relations are employed to describe how a compressing map extracts the same output from distinct sequences. The reader is referred to [5] for more about relations.

Let \mathbb{Z} be the set of integers. A *sequence* \vec{s} over a set A is a map $\vec{s} : \mathbb{Z} \rightarrow A$. Denote the set of sequences over A by A^∞ . Then a map $\psi : A \rightarrow B$ naturally induces a map $\hat{\psi} : A^\infty \rightarrow B^\infty$ defined by $\hat{\psi}(\vec{s}) = \psi \circ \vec{s}$.

A (*binary*) *relation* R on a set A is a subset of $A \times A$. The relation R is *reflexive* if $(a, a) \in R$ for any $a \in A$; R is *symmetric* if $(a_1, a_2) \in R$ implies $(a_2, a_1) \in R$ for any $a_1, a_2 \in A$; R is *transitive* if $(a_1, a_2) \in R$ and $(a_2, a_3) \in R$ imply $(a_1, a_3) \in R$ for any $a_1, a_2, a_3 \in A$. The *transitive closure* of R is the smallest transitive relation including R , denoted by $R^{(T)}$. A relation that is reflexive, symmetric and transitive is an *equivalence relation*. If R is an equivalence relation on A , then the *equivalence class* of $a \in A$ is the set $\{b : (a, b) \in R\}$. The *equivalence closure* of R is the smallest equivalence relation including R , denoted by $R^{(E)}$. A *partition* \mathcal{P} of A is a set of pairwise disjoint nonempty sets whose union is A . Actually, there is a canonical one-one correspondence between

equivalence relations on A and partitions of A . Denote by $\mathcal{P}(R)$ the partition determined by $R^{(E)}$, i.e. $\mathcal{P}(R) = \{ \{a : (a, b) \in R^{(E)}\} : b \in A \}$.

Let ψ be a map defined on A . Then ψ defines an equivalence relation $\{(a_1, a_2) \in A \times A : \psi(a_1) = \psi(a_2)\}$, denoted by R^ψ . We call ψ to be *constant on* $B \subset A$ if $\psi(b_1) = \psi(b_2)$ for any $b_1, b_2 \in B$; and ψ is said to *admit* a partition \mathcal{P} of A if ψ is constant on any set in \mathcal{P} .

Fact 1. *For an equivalence relation R on A , $R \subset R^\psi$ if and only if ψ admits $\mathcal{P}(R)$.*

Given two sequences \vec{s}_1 and \vec{s}_2 over A , define a relation on A by

$$R_A(\vec{s}_1, \vec{s}_2) = \{(\vec{s}_1(i), \vec{s}_2(i)) \in A \times A : i \in \mathbb{Z}\}.$$

By definition, $\widehat{\psi}(\vec{s}_1) = \widehat{\psi}(\vec{s}_2)$ if and only if $\psi(a_1) = \psi(a_2)$ for any $(a_1, a_2) \in R_A(\vec{s}_1, \vec{s}_2)$, i.e. $R_A(\vec{s}_1, \vec{s}_2) \subset R^\psi$, that is $R_A(\vec{s}_1, \vec{s}_2)^{(E)} \subset R^\psi$ because R^ψ is per se an equivalence relation.

Fact 2. *Let $\vec{s}_1, \vec{s}_2 \in A^\infty$. Then a map ψ defined on A satisfies $\widehat{\psi}(\vec{s}_1) = \widehat{\psi}(\vec{s}_2)$ if and only if $R_A(\vec{s}_1, \vec{s}_2)^{(E)} \subset R^\psi$.*

2.3 Galois rings

This subsection presents notations about p -adic rings and Galois rings. More about p -adic rings is available in [20, 21].

For a ring A , the multiplicative group of invertible elements is denoted by A^* . For $S \subset A$ and $a \in A$, denote $a + S = \{a + b : b \in S\}$ and $aS = \{ab : b \in S\}$. For $S_1, S_2 \subset A$, denote $S_1 + S_2 = \{a + b : a \in S_1, b \in S_2\}$.

Let \mathbb{Z}_p be the ring of p -adic integers, and let O be an unramified extension of \mathbb{Z}_p of degree n . For $e > 0$, denote $A_e = \mathbb{Z}_p/p^e\mathbb{Z}_p$ and $O_e = O/p^eO$, where $A_\infty = \mathbb{Z}_p$ and $O_\infty = O$. Always suppose $\sigma(x) \bmod p$ to be irreducible over \mathbb{F}_p , and take $O_e = A_e[x]/(\sigma(x))$. Since O_e/pO_e , as an additive group, is isomorphic to \mathbb{F}_q , we denote $\bar{z} = z \bmod p \in \mathbb{F}_q$ for $z \in O_e$.

The discrete valuation on O_e is defined as $v(z) = \max\{m \leq e : z \in p^m O_e\}$ for $z \in O_e$. Given $\gamma \in O_e^*$, define $r(\gamma) = \max\{v(\gamma - z) : z \in A_e\}$ and also a partition of A_e by

$$\mathcal{C}_\gamma = \left\{ \{z\gamma^i : i \in \mathbb{Z}\} + p^{r(\gamma)} A_e : z \in A_e \right\}.$$

From now on let W be the set of $(q-1)$ -th roots of unity in O_e and $U_e = 1 + pO_e$. Let η be a root of $\sigma(x)$ throughout. Due to the direct product $O_e^* = W \times U_e$, η is uniquely factorized as $\eta = \zeta u$, where $\zeta \in W$ and $u \in U_e$. As a multiplicative group, W is isomorphic to \mathbb{F}_q^* . Always denote $u_1 = (u-1)/p$ and

$$\delta = \begin{cases} (u-1)/p, & \text{if } p \geq 3, \\ (u^2-1)/4, & \text{if } e > p = 2, \\ (u-1)/p, & \text{if } e = p = 2. \end{cases}$$

Due to the Krull topology, an element of O_e (resp. A_e) is, roughly speaking, considered as an element of O (resp. \mathbb{Z}_p) only pruned up to the e -level precision. For example, $r(\gamma)$ tells the finest precision at which γ belongs to \mathbb{Z}_p . Furthermore, a continuous map under the Krull topology is commutative with pruning to any precision. In this article only addition, multiplication and trace are involved and all of them are continuous w.r.t. the Krull topology. Thereby, without ambiguity we denote the trace function of O_e over R_e by tr for any $e \geq 1$.

2.4 Primitive sequences over A_e

Above all, sequences generated by $\sigma(x)$ can be parameterized by trace functions. Here we omit the detailed reasoning, which is the same as in [13, Chap.8], only substituting p -adic rings for finite fields. A sequence generated by $\sigma(x)$ can be parameterized by $\alpha \in O_e$ as $\vec{s}_\alpha : \vec{s}_\alpha(t) = \text{tr}(\alpha \eta^t)$, and its set of LFSR-states is $S_\alpha = \{\alpha \eta^t : t \in \mathbb{Z}\} = \{\alpha \zeta^i u^j : i, j \in \mathbb{Z}\}$. Denote $G_e(\eta) = \{\vec{s}_\alpha : \alpha \in O_e^*\}$.

For $a, b \in \mathbb{Z}_p$ and a relation R on A_i , without ambiguity we simply write $(a, b) \in R$ instead of $(a \bmod p^i, b \bmod p^i) \in R$. Given $\alpha, \beta \in O^*$, for simplicity we denote $S_\alpha^b = \{z \in S_\alpha : \text{tr}(z\delta) \not\equiv 0 \bmod p\}$ and two relations on A_i :

$$\begin{aligned} R_i(\alpha, \beta) &= \{(\text{tr}(z), \text{tr}(z\beta/\alpha)) : z \in S_\alpha\}; \\ R_i^b(\alpha, \beta) &= \{(\text{tr}(z), \text{tr}(z\beta/\alpha)) : z \in S_\alpha^b\}. \end{aligned}$$

Clearly, $S_\alpha^b \subset S_\alpha$ and $R_i^b(\alpha, \beta) \subset R_i(\alpha, \beta)$.

Fact 3. For $a, b \in \mathbb{Z}_p$, $(a, b) \in R_i(\alpha, \beta)$ means exactly that there exist $a', b' \in \mathbb{Z}_p$ satisfying $a' \equiv a \bmod p^{i+1}$, $b' \equiv b \bmod p^{i+1}$, and $(a', b') \in R_{i+1}(\alpha, \beta)$.

The rest of this subsection was given by [2, 7, 15] in the language of polynomials, and now will be reinterpreted in the language of p -adic rings. For $z \in O_e^*$, denote $o(\bar{z}) = \min\{i > 0 : z^i \equiv 1 \bmod p\}$, i.e. the order of \bar{z} in \mathbb{F}_q^* . The polynomial $\sigma(x)$ (or a sequence $\vec{s} \in G_e(\eta)$) is said to be *primitive* if $o(\bar{\zeta}) = q - 1$ and $\bar{\delta} \neq 0$; the polynomial $\sigma(x)$ (or a sequence $\vec{s} \in G_e(\eta)$) is said to be *strongly primitive* if $o(\bar{\zeta}) = q - 1$ and $r(\delta) = 0$.

Remark 1. When $p \geq 3$ or $e = p = 2$, strong primitivity implies that 1 and $\bar{\delta}$ are linear independent over \mathbb{F}_p . When $e > p = 2$, we have $\bar{\delta} = \bar{u}_1^2 + \bar{u}_1$; primitivity implies $r(u) = 1$, i.e. $\bar{u}_1 \notin \mathbb{F}_2$; and strong primitivity implies that 1, \bar{u}_1 , $\bar{\delta}$ are linear independent over \mathbb{F}_2 . Thus, there exist no strongly primitive polynomials if $e > p = n = 2$. If $p = 2$ and $2 \nmid n$, then $\sigma(x)$ is strongly primitive if and only if $\sigma(x)$ is primitive [15].

3 Main results

For all that follows $\vec{s}_\alpha, \vec{s}_\beta \in G_e(\eta)$ and $\gamma = \beta/\alpha \neq 1$.

Remark 2. To compute γ , one needs only consecutive n outputted data in \vec{s}_α and \vec{s}_β rather than α and β .

Condition 1. It holds that $p \geq 3$, $r(\gamma) = r(\delta) = 0$, $r(\delta^2) \geq 1$ and $r(\delta/\gamma) \geq 1$.

Remark 3. Condition 1 exactly means that $\bar{\gamma}$ and $\bar{\delta}$ are \mathbb{F}_p -linear dependent and either of them is an irrational square root. Hence, if n is odd or $\sigma(x)$ is not strongly primitive, then Condition 1 does not hold. Condition 1 excludes $p = 2$ because $r(\delta) = r(\delta^2)$ if $p = 2$. Therefore, if $p \geq 3$ and n is even, then only $(p-1)/(p^n-p)$ of strongly primitive polynomials do not satisfy Condition 1.

Theorem 1. Let $p \geq 3$ or $e = p = 2$. Suppose that $\sigma(x)$ is primitive and $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$. Then one of the following three cases occurs: (i) ψ is constant on $a + p^{e-1}A_e$ for any $a \in A_e^*$ if Condition 1 does

not hold; (ii) ψ is constant on $a + p^{e-1}A_e$ for any $a \in A_e^*$ or for any $a \in pA_e$ if Condition 1 holds; (iii) $\gamma^m \equiv 1 \pmod{p^e}$, where m is a prime divisor of $p-1$, and ψ is constant on $\{\gamma^i : 1 \leq i \leq m\}$ for any $a \in A_e^*$ (for any $a \in A_e$ if $\sigma(x)$ is strongly primitive).

Theorem 2. Let p be an odd prime and let ψ be a map on A_e . Suppose that $\sigma(x)$ is primitive and $\bar{\delta}^2 \notin \mathbb{F}_p$. Then $\hat{\psi}$ is injective on $G_e(\eta)$ if and only if for any m -th root of unity $\gamma \in A_e$, where m is a prime divisor of $p-1$, there exists $a \in A_e$ such that ψ is not constant on $\{\gamma^i a : 1 \leq i \leq m\}$.

Remark 4. In Theorem 2, $\bar{\delta}^2 \notin \mathbb{F}_p$, translated into the language of polynomials, is exactly $(x^{q-1} - 1)^2 / p^2 \not\equiv a \pmod{(p, \sigma(x))}$ for any $a \in \mathbb{F}_p$. In fact, only $(3 + (-1)^n)(p-1)/(2(q-1))$ of primitive polynomials satisfy $\bar{\delta}^2 \in \mathbb{F}_p$.

Remark 5. Given a finite set S and conditions in Theorem 2, the number of entropy-preserving maps on S can be estimated as below. Denote $\tau(m) = e_1 + e_2 + \dots + e_k$ for $m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, where p_1, p_2, \dots, p_k are positive prime integers; Particularly, $\tau(1) = 0$. Define $\rho(m) = |S|^{(1+(p^e-1)/m)}$ for $0 < m \mid (p-1)$. Then the number of entropy-preserving maps from A_e to S is

$$N = \sum_{m \mid p-1} (-1)^{\tau(m)} \rho(m).$$

Therefore, the proportion of entropy-preserving maps in all maps from A_e to S is

$$N/|S|^{p^e} > 1 - \log p |S|^{(1-p^e)/2},$$

sharply approaching to 1 when either p or e increases.

The proof of Theorem 1 and Theorem 2 will be given at the end of this section.

By Fact 1 and Fact 2, the key to decide distinctness of compressed sequences $\hat{\psi}(\vec{s}_\alpha)$ and $\hat{\psi}(\vec{s}_\beta)$ is determining $\mathcal{P}(R_e(\alpha, \beta))$.

Later we need the following lemma frequently.

Lemma 3. Let $z \in S_\alpha$. Assume $2 \leq i \leq e$ if $p \geq 3$ or $p = e = 2$; $3 \leq i \leq e$ if $e > p = 2$. Then for any $j \in \mathbb{Z}$,

$$(\text{tr}(z) + jp^{i-1}\text{tr}(z\delta), \text{tr}(\gamma z) + jp^{i-1}\text{tr}(z\gamma\delta)) \in R_i(\alpha, \beta).$$

Particularly, if $r(\gamma) \geq 1$ and $(v_1, v_2) \in R_i^b(\alpha, \beta)$, then $(v_1 + jp^{i-1}, v_2 + jp^{i-1}\gamma) \in R_i^b(\alpha, \beta)$ for any $j \in \mathbb{Z}/p\mathbb{Z}$.

Proof. Notice that $(\text{tr}(zu^{jp^{i-2}}), \text{tr}(\gamma zu^{jp^{i-2}})) \in R_i(\alpha, \beta)$. Since $u^{jp^{i-2}} \equiv 1 + jp^{i-1}\delta \pmod{p^i}$, we have

$$\begin{aligned} \text{tr}(zu^{jp^{i-2}}) &\equiv \text{tr}(z) + jp^{i-1}\text{tr}(z\delta) \pmod{p^i}, \\ \text{tr}(\gamma zu^{jp^{i-2}}) &\equiv \text{tr}(\gamma z) + jp^{i-1}\text{tr}(z\gamma\delta) \pmod{p^i}. \end{aligned}$$

If $r(\gamma) \geq 1$ and $(v_1, v_2) \in R_i^b(\alpha, \beta)$, we use $\text{tr}(z\gamma\delta) \equiv \gamma\text{tr}(z\delta) \not\equiv 0 \pmod{p}$. □

3.1 Finite field case

In this subsection we consider $e = 1$, i.e. $O_1 = \mathbb{F}_q$. In this case a primitive sequence is actually a well-known m -sequence [13], and $G_1(\eta)$ is the set of m -sequences generated by Eq.(1) over \mathbb{F}_p .

By Lemma 2, $\mathcal{P}(R_e(\alpha, \beta)) = \mathcal{C}_\gamma$. Specifically, if $\gamma \in \mathbb{F}_q^* \setminus \mathbb{F}_p$, $\mathcal{C}_\gamma = \{\mathbb{F}_p\}$; if $\gamma \in \mathbb{F}_p^*$, $\mathcal{C}_\gamma = \{\{a\gamma^i : i \in \mathbb{Z}\} : a \in \mathbb{F}_p\}$. Then noticing that \mathbb{F}_p^* is a cyclic group of order $p - 1$, we have

Theorem 3. *Let ψ be a map defined on \mathbb{F}_p . For two distinct m -sequences \vec{s}_α and \vec{s}_β , ψ satisfies $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$ if and only if ψ admits \mathcal{C}_γ . Furthermore, $\widehat{\psi}$ is injective on $G_1(\eta)$ if and only if for any prime divisor m of $p - 1$ and for any map f on \mathbb{F}_p $\psi(z) \neq f(z^m)$.*

In the rest of this article we only consider $e \geq 2$.

3.2 Occurring elements

In this subsection we study $\{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$, i.e. the elements of A_e occurring in \vec{s}_α .

Lemma 4. *Assume (i) $p \geq 3$ or $e = p = 2$, and $\nu \in S_\alpha^b$; or (ii) $e > p = 2$ and $\nu \in S_\alpha^b$ satisfying $\text{tr}(\nu u_1) \equiv 1 \pmod{2}$. Then for any $a \in \text{tr}(\nu) + p^m A_e$, $m \geq 1$, there exists a unique $z \in \{\nu u^{p^{m-1}j} : j \in \mathbb{Z}\}$ satisfying $\text{tr}(z) = a$.*

Proof. Suppose $a - \text{tr}(\nu) \in p^i R_e$ for some $i \geq m$. Denote $z_i = \nu$. Since $\text{tr}(z_i \delta) \equiv \text{tr}(\nu \delta) \not\equiv 0 \pmod{p}$ and

$$u^{p^{i-1}j} \equiv 1 + jp^i \delta \pmod{p^{i+1}}$$

for $1 \leq i \leq e$ when $p \geq 3$ or $e = p = 2$, or for $2 \leq i \leq e$ when $e > p = 2$, we take

$$j \equiv (a - \text{tr}(z_i))(\text{tr}(\nu \delta))^{-1}/p^i \pmod{p}$$

and $z_{i+1} = z_i u^{p^{i-1}j}$, yielding

$$\text{tr}(z_{i+1}) \equiv \text{tr}(z_i) + jp^i \text{tr}(\nu \delta) \equiv a \pmod{p^{i+1}}.$$

Unless $m = 1$ and $e > p = 2$, using induction on i gives $z = z_e \in \{\nu u^{p^{m-1}j} : j \in \mathbb{Z}\}$ with $\text{tr}(z) = a$. Finally, for $m = 1$ and $e > p = 2$, due to $\text{tr}(u_1 \nu) \equiv 1 \pmod{2}$, similar to the proof for case $e = p = 2$, we have $z_2 \in \{\nu, \nu u\}$ with $\text{tr}(z_2) \equiv a \pmod{4}$. Then the induction above is also valid. \square

Theorem 4. *Let $\vec{s}_\alpha \in G_e(\eta)$. If $\sigma(x)$ is primitive, then $\{\vec{s}_\alpha(i) : i \in \mathbb{Z}\} \supset A_e^*$. If $\sigma(x)$ is strongly primitive, then $\{\vec{s}_\alpha(i) : i \in \mathbb{Z}\} = A_e$.*

Proof. Choose any $a \in A_e$.

Suppose $p \geq 3$ or $e = p = 2$. If there exists z satisfying

$$\begin{cases} \text{tr}(z) & \equiv a \pmod{p}, \\ \text{tr}(z\delta) & \not\equiv 0 \pmod{p}, \end{cases} \quad (5)$$

then by Lemma 4, $a \in \{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$.

Suppose $e > p = 2$. Similarly, if there exists z satisfying

$$\begin{cases} \operatorname{tr}(z) & \equiv a \pmod{2}, \\ \operatorname{tr}(zu_1) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(z\delta) & \equiv 1 \pmod{2}, \end{cases} \quad (6)$$

then by Lemma 4, $a \in \{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$.

Finally, by Remark 1 and Lemma 1, if $\sigma(x)$ is strongly primitive and $a \in A_e$, or if $\sigma(x)$ is primitive and $a \in A_e^*$, then Eq.(5) and Eq.(6) are solvable. \square

There exists $\vec{s} \in G_e(\eta)$ with $\{\vec{s}(i) : i \in \mathbb{Z}\} \subsetneq A_e$, and below is such an example.

Example 1. Take $e = p = 3$. Denote by w a root of the polynomial $x^2 + 2x + 2$ over $\mathbb{Z}/27\mathbb{Z}$. Let $\eta = 5w + 1$, then $u \equiv -2 \pmod{9}$. The minimal polynomial of η is $x^2 + 8x - 13$, and it is primitive, but not strongly primitive. For the sequence $\vec{s}(i) = -\operatorname{tr}((12w + 13)\eta^i)$, $\{\vec{s}(i) : i \in \mathbb{Z}\} = \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 7, \pm 8, \pm 10, \pm 11, \pm 13\}$.

3.3 Case $r(\gamma) = 0$

Lemma 5. Let $r(\gamma) = 0$. If Condition 1 holds, then $pA_e \subset S$ for some $S \in \mathcal{P}(R_e(\alpha, \beta))$. Suppose that Condition 1 does not hold. If $\sigma(x)$ is primitive and $p \geq 3$ (or $e = p = 2$), then $A_e^* \subset S$ for some $S \in \mathcal{P}(R_e(\alpha, \beta))$. If $\sigma(x)$ is primitive and $e > p = 2$, then either $A_e^* \subset S$ for some $S \in \mathcal{P}(R_e(\alpha, \beta))$ or $2A_e \subset S$ for some $S \in \mathcal{P}(R_e(\alpha, \beta))$. If $\sigma(x)$ is strongly primitive, then $\mathcal{P}(R_e(\alpha, \beta)) = \{A_e\}$.

Proof. For simplicity we call $a \in \mathbb{Z}_p$ to be *good* for $R_i(\alpha, \beta)$ if there exists $b \in \mathbb{Z}_p$ such that $(a + jp^{i-1}, b) \in R_i(\alpha, \beta)$ for any $j \in \mathbb{Z}$, or $(b, a + jp^{i-1}) \in R_i(\alpha, \beta)$ for any $j \in \mathbb{Z}$. Clearly, if a is good for $R_i(\alpha, \beta)$, then $(a, a + jp^{i-1}) \in R_i(\alpha, \beta)^{(E)}$ for any $j \in \mathbb{Z}$.

Let $B_i^g \subset \{\operatorname{tr}(z) : z \in S_\alpha^b \cap S_\beta^b\}$ satisfy that each element of B_i^g is good for $R_e(\alpha, \beta)$ and $\{a \pmod{p^i} : a \in B_{i+1}^g\} \subset B_i^g$ for any $i > 0$. Use induction on i to show $B_e^g \subset S$ for some $S \in \mathcal{P}(R_e(\alpha, \beta))$. By Lemma 2, $\mathcal{P}(R_1(\alpha, \beta)) = \{\mathbb{F}_p\}$. Assume that the proof is done for i , and below we show $B_{i+1}^g \subset S$ for some $S \in \mathcal{P}(R_{i+1}(\alpha, \beta))$. Choose any $b_0, b_1 \in B_{i+1}^g$. Since $B_{i+1}^g/p^i B_{i+1}^g \subset B_i^g$, we have $(b_0, b_1) \in R_i(\alpha, \beta)^{(E)}$. By Fact 3, there exists $z_0, z_1 \in A_{i+1}$ such that $z_0 \equiv b_0 \pmod{p^{i+1}}$, $z_1 \equiv b_1 \pmod{p^{i+1}}$, and $(z_0, z_1) \in R_{i+1}(\alpha, \beta)^{(E)}$. Since b_0, b_1 are good for $R_{i+1}(\alpha, \beta)$, we have $(z_0, b_0) \in R_{i+1}(\alpha, \beta)^{(E)}$ and $(z_1, b_1) \in R_{i+1}(\alpha, \beta)^{(E)}$. By transitivity of $R_{i+1}(\alpha, \beta)^{(E)}$, we have $(b_0, b_1) \in R_{i+1}(\alpha, \beta)^{(E)}$. Thus, $B_{i+1}^g \subset S$ for some $S \in \mathcal{P}(R_{i+1}(\alpha, \beta))$.

Furthermore, if for any $a \in A_e \setminus B_e^g$ there is $b \in B_e^g$ with $(a, b) \in R_e(\alpha, \beta)^{(E)}$, then $\{A_e\} = \mathcal{P}(R_e(\alpha, \beta))$ by transitivity.

The rest of proof is explicitly presenting B_e^g with properties required above.

Case $p \geq 3$ or $e = p = 2$.

If there exists w satisfying

$$\begin{cases} \operatorname{tr}(w) & \equiv a \pmod{p}, \\ \operatorname{tr}(\delta w) & \not\equiv 0 \pmod{p}, \\ \operatorname{tr}(\gamma \delta w) & \equiv 0 \pmod{p}, \end{cases} \quad (7)$$

by Lemma 4 there exists $z \in S_\alpha^b$ such that $\text{tr}(z) = a$ and $\text{tr}(z\gamma\delta) \equiv 0 \pmod{p}$. By Lemma 3, $(a + jp^{e-1}, \text{tr}(z\gamma)) \in R_e(\alpha, \beta)$ for any $j \in \mathbb{Z}/p\mathbb{Z}$. Hence, a is good for $R_e(\alpha, \beta)$. If there exists w satisfying

$$\begin{cases} \text{tr}(\gamma w) & \equiv a & \pmod{p}, \\ \text{tr}(\gamma\delta w) & \not\equiv 0 & \pmod{p}, \\ \text{tr}(\delta w) & \equiv 0 & \pmod{p}, \end{cases} \quad (8)$$

by Lemma 4, there exists $z \in S_\beta^b$ satisfying $\text{tr}(z) = a$ and $\text{tr}(z\delta/\gamma) \equiv 0 \pmod{p}$. By Lemma 3, $(\text{tr}(z/\gamma), a + jp^{e-1}) \in R_e(\alpha, \beta)$ for any $j \in \mathbb{Z}/p\mathbb{Z}$. Hence, a is good for $R_e(\alpha, \beta)$.

Suppose that $\sigma(x)$ is strongly primitive and Condition 1 does not hold. (i) If $1, \bar{\delta}$ and $\bar{\gamma}\bar{\delta}$ are linear independent over \mathbb{F}_p , then Eq.(7) is solvable. (ii) If $\bar{\gamma}, \bar{\delta}$ and $\bar{\gamma}\bar{\delta}$ are linear independent over \mathbb{F}_p , then Eq.(8) is solvable. (iii) If $\bar{\gamma}\bar{\delta} = r_0 + r_1\bar{\delta}$, $r_1 \neq 0$, then there exists w satisfying $\text{tr}(w) = \bar{a}$ and $\text{tr}(\delta w) = -r_0\bar{a}/r_1$, and hence $\text{tr}(\gamma\delta w) = 0$. Thus, if $\bar{a} \neq 0$, there exists $w \in O^*$ satisfying Eq.(7). (iv) If $\bar{\delta} = r_0\bar{\gamma} + r_1\bar{\gamma}\bar{\delta}$, $r_1 \neq 0$, then there exists w satisfying $\text{tr}(\gamma w) = \bar{a}$ and $\text{tr}(\gamma\delta w) = -r_0\bar{a}/r_1$, and hence $\text{tr}(\delta w) = 0$. Thus, if $\bar{a} \neq 0$, there exists w satisfying Eq.(8). If none of cases (i),(ii),(iii),(iv) holds, then Condition 1 is true. Therefore, if $\sigma(x)$ is strongly primitive and Condition 1 does not hold, then any $a \in \mathbb{Z}_p^*$ is good for $R_e(\alpha, \beta)$. Thus, we take $B_e^g = A_e^*$. Furthermore, since $1, \bar{\delta}$ are linear independent over \mathbb{F}_p and $1, \bar{\gamma}$ are linear independent over \mathbb{F}_p ,

$$\begin{cases} \text{tr}(w) & \equiv 0 & \pmod{p}, \\ \text{tr}(w\delta) & \not\equiv 0 & \pmod{p}, \\ \text{tr}(w\gamma) & \not\equiv 0 & \pmod{p}, \end{cases}$$

is solvable. By Lemma 4, for any $a \in pA_e$ there exists $b \in \mathbb{Z}_p^*$ good for $R_e(\alpha, \beta)$ satisfying $(a, b) \in R_e(\alpha, \beta) \subset R_e(\alpha, \beta)^{(E)}$.

Now suppose that $\sigma(x)$ is primitive but not strongly primitive. Since $\bar{\delta} \in \mathbb{F}_p^*$, Eq.(7) is equivalent to

$$\begin{cases} \text{tr}(w) & \equiv a \not\equiv 0 & \pmod{p}, \\ \text{tr}(\gamma w) & \equiv 0 & \pmod{p}, \end{cases}$$

which is solvable since $\bar{\gamma} \notin \mathbb{F}_p$. Hence, any $a \in A_e^*$ is good for $R_e(\alpha, \beta)$ and we also take $B_e^g = A_e^*$.

Now suppose that Condition 1 holds. For $a \in pA_e$, Eq.(7) is equivalent to

$$\begin{cases} \text{tr}(w) & \equiv 0 & \pmod{p}, \\ \text{tr}(\delta w) & \not\equiv 0 & \pmod{p}, \end{cases}$$

which is solvable since $\bar{\delta} \notin \mathbb{F}_p$. Hence, any $a \in pA_e$ is good for $R_e(\alpha, \beta)$ and take $B_e^g = pA_e$.

Case $e > p = 2$. Recall $u_1 = (u - 1)/2$.

Assume that $\sigma(x)$ is strongly primitive. By Remark 1, $n \geq 3$. Similar to the proof of case $p \geq 3$, if there exists w satisfying

$$\begin{cases} \text{tr}(w) & \equiv a & \pmod{2}, \\ \text{tr}(u_1 w) & \equiv 1 & \pmod{2}, \\ \text{tr}(\delta w) & \equiv 1 & \pmod{2}, \\ \text{tr}(\gamma\delta w) & \equiv 0 & \pmod{2}, \end{cases}$$

or

$$\begin{cases} \operatorname{tr}(\gamma w) & \equiv a \pmod{2}, \\ \operatorname{tr}(u_1 \gamma w) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(\gamma \delta w) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(\delta w) & \equiv 0 \pmod{2}, \end{cases}$$

then a is good for $R_e(\alpha, \beta)$. Equivalently, it is sufficient to consider

$$\begin{cases} \operatorname{tr}(w) & \equiv a \pmod{2}, \\ \operatorname{tr}(u_1 w) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(\delta w) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(w \gamma \delta) \operatorname{tr}(w \delta / \gamma) & \equiv 0 \pmod{2}. \end{cases} \quad (9)$$

Recall that $1, \overline{u_1}$ and $\overline{\delta}$ are linear independent over \mathbb{F}_2 . If $\overline{\delta \gamma}$ or $\overline{\delta / \gamma}$ is not linear representable by $1, \overline{u_1}$ and $\overline{\delta}$, then Eq.(9) is solvable and any $a \in A_e$ is good for $R_e(\alpha, \beta)$. If so, we take $B_e^g = A_e^*$ for $e \geq 1$. If $\overline{\delta \gamma}$ is not linear representable by $1, \overline{u_1}$ and $\overline{\delta}$, then $1, \overline{u_1}, \overline{\gamma u_1}$ are independent over \mathbb{F}_2 and Eq.(7) is solvable for $e = 2$; if $\overline{\delta / \gamma}$ is not linear representable by $1, \overline{u_1}$ and $\overline{\delta}$, then $\overline{\gamma}, \overline{u_1}, \overline{\gamma u_1}$ are independent over \mathbb{F}_2 and Eq.(8) is solvable for $e = 2$; thus, B_2^g is well-defined. Provided with $\overline{\delta} = \overline{u_1^2} + \overline{u_1} \notin \mathbb{F}_2$, by solving

$$\begin{cases} a_0 a + a_1 + a_2 & = 1, \\ b_0 a + b_1 + b_2 & = 1, \\ a_0 + a_1 \overline{u_1} + a_2 \overline{\delta} & = \overline{\delta \gamma}, \\ b_0 + b_1 \overline{u_1} + b_2 \overline{\delta} & = \overline{\delta / \gamma}, \end{cases}$$

where $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{F}_2$, in Table 1 we list all cases in which Eq.(9) has no solution. In Table 1 the last column f_{u_1} shows the minimal polynomial of $\overline{u_1}$ over \mathbb{F}_2 . For any fixed u_1 and γ in Table

Table 1: Cases: Eq.(9) is not solvable

\overline{a}	a_0	a_1	a_2	b_0	b_1	b_2	$\overline{\gamma}$	$1/\overline{\gamma}$	$\operatorname{tr}(w\gamma)$	$\operatorname{tr}(w/\gamma)$	f_{u_1}
0	0	1	0	1	0	1	$\overline{u_1^2}$	$1 + \overline{u_1}$	0	1	$x^3 + x^2 + 1$
0	1	0	1	0	1	0	$1 + \overline{u_1}$	$\overline{u_1^2}$	1	0	$x^3 + x^2 + 1$
0	1	0	1	1	1	0	$\overline{u_1}$	$1 + \overline{u_1^2}$	1	0	$x^3 + x + 1$
0	1	1	0	1	0	1	$1 + \overline{u_1^2}$	$\overline{u_1}$	0	1	$x^3 + x + 1$
1	0	1	0	1	0	0	$\overline{u_1^2} + \overline{u_1}$	$1 + \overline{u_1}$	1	0	$x^3 + x + 1$
1	1	0	0	0	1	0	$1 + \overline{u_1}$	$\overline{u_1} + \overline{u_1^2}$	0	1	$x^3 + x + 1$

$1, \overline{a}$ does not occur both as 0 and as 1, implying that either any $a \in A_e^*$ is good for $R_e(\alpha, \beta)$ or any $a \in 2A_e$ is good for $R_e(\alpha, \beta)$. For the case $\overline{a} = 1$ in Table 1 we take $B_e^g = 2A_e$ for $e \geq 1$. For the case $\overline{a} = 0$ in Table 1 we take $B_e^g = A_e^*$ for $e \geq 1$. For each case in Table 1, either $1, \overline{u_1}, \overline{\gamma u_1}$ are independent over \mathbb{F}_2 and Eq.(7) is solvable, or $\overline{\gamma}, \overline{u_1}, \overline{\gamma u_1}$ are independent over \mathbb{F}_2 and Eq.(8) is solvable. Thus, B_2^g is well-defined. Simultaneously, for each case in Table 1 either $\operatorname{tr}(w\gamma) = 1 + \overline{a}$ or $\operatorname{tr}(w/\gamma) = 1 + \overline{a}$, implying there exists b good for $R_e(\alpha, \beta)$ satisfying $(a, b) \in R_e(\alpha, \beta)^{(E)}$.

Assume that $\sigma(x)$ is primitive but not strongly primitive. Then $\bar{\delta} = \overline{u_1^2} + \overline{u_1} = 1$. For $a \in A_e^*$, Eq.(9) is equivalent to

$$\begin{cases} \operatorname{tr}(w) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(u_1 w) & \equiv 1 \pmod{2}, \\ \operatorname{tr}(w\gamma) \operatorname{tr}(w/\gamma) & \equiv 0 \pmod{2}, \end{cases}$$

which is always solvable since in our scenario

$$\begin{cases} a_0 + a_1 & = 1, \\ b_0 + b_1 & = 1, \\ a_0 + a_1 \overline{u_1} & = \overline{\gamma}, \\ b_0 + b_1 \overline{u_1} & = 1/\overline{\gamma}, \end{cases}$$

has no solution, where $a_0, a_1, b_0, b_1 \in \mathbb{F}_2$. Thus, any $a \in \mathbb{Z}_2^*$ is good for $R_e(\alpha, \beta)$ and take $B_e^g = A_e^*$. Under this case either Eq.(7) or Eq.(8) is solvable for $a \in A_2$ and hence B_2^g is also well-defined.

Each element of B_e^g is good for $R_e(\alpha, \beta)$, and $\{a \pmod{p^e} : a \in B_{e+1}^g\} = B_e^g$. By Theorem 4, $B_e^g \subset \{\operatorname{tr}(z) : z \in S_\alpha^b \cap S_\beta^b\}$. \square

By Fact 1, Fact 2 and Lemma 5,

Theorem 5. *Let $\vec{s}_\alpha, \vec{s}_\beta \in G_e(\eta)$ and $r(\gamma) = 0$. Let ψ be a map defined on A_e . If Condition 1 holds and $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$, then ψ is constant on pA_e . Suppose that Condition 1 does not hold. If $\sigma(x)$ is strongly primitive, then $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$ if and only if ψ is constant on A_e . If $\sigma(x)$ is primitive, $p \geq 3$ (or $e = p = 2$) and $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$, then ψ is constant on A_e^* . If $\sigma(x)$ is primitive, $e > p = 2$ and $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$, then ψ is constant on A_e^* or ψ is constant on pA_e .*

Below is an example under Condition 1.

Example 2. Choose $p = 3$, $e = n = 2$, and let w be a root of $x^2 + 2x + 2$. Furthermore, $\eta = w - 4$ and $\delta = w + 1$. See $\delta^2 = -1$. Let $\alpha = 1$ and $\beta = w + 1$. Then

$$\mathcal{P}(R_2(\alpha, \beta)) = \{\{\pm 4\}, \{0, \pm 1, \pm 2, \pm 3\}\}.$$

Actually, the example in [27, Remark 8] also satisfies Condition 1.

It remains interesting to consider whether the following conjecture is true.

Conjecture 1. *If Condition 1 is true, then $\mathcal{P}(R_e(\alpha, \beta)) = \{A_e\}$ when the extension degree n of O over \mathbb{Z}_p is large enough.*

3.4 Case $r(\gamma) \geq 1$

A subset $S \subset \mathbb{Z}_p$ is said to be *bold* in $R_i(\alpha, \beta)$ if $(v_1, v_2) \in R_i^b(\alpha, \beta)^{(T)}$ for any $v_1, v_2 \in S$.

The key fact we need is

Lemma 6. *Suppose $p \geq 3$ or $r(\gamma) \geq 2$. Let $\sigma(x)$ be primitive and $1 \leq r(\gamma) < e$. If $S + p^{e-1}\mathbb{Z}_p \subset S$ and S is bold in $R_e(\alpha, \beta)$, then S is also bold in $R_{e+1}(\alpha, \beta)$.*

Proof. Let $\gamma = \gamma_0(1 + \gamma_\ell p^\ell)$, where $\ell = r(\gamma)$, i.e. $\gamma_0 \in \mathbb{Z}_p$ and $\gamma_\ell \in O^* \setminus \mathbb{Z}_p$.

Choose any $a \in S$. Since $S + p^{e-1}\mathbb{Z}_p$ is bold in $R_e(\alpha, \beta)$, by Lemma 4 and Fact 3, there exist $z_{0,0}, z_{1,0}, \dots, z_{m,0} \in S_\alpha^b$ such that $\text{tr}(z_{0,0}) \equiv a \pmod{p^{e+1}}$, $\text{tr}(z_{m,0}) - \text{tr}(z_{0,0}) \in p^{e-1}\mathbb{Z}_p^*$, and $\text{tr}(z_{i,0}) \equiv \text{tr}(\gamma z_{i-1,0}) \pmod{p^{e+1}}$, $i = 1, 2, \dots, m$. Denote $\Delta = \text{tr}(z_{m,0}) - \text{tr}(z_{0,0})$. By Lemma 4, we can choose $z_{m,0} \in z_{0,0} + p^{e-1}O^*$. Notice that $\gamma_0^m \in 1 + p^\ell\mathbb{Z}_p$.

For $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, p-1$, iteratively define

$$\begin{cases} z_{0,j} &= z_{m,j-1} \pmod{p^{e+1}}, \\ z_{i,j} &= z_{i,0} u^{(jt_i + k_{i,j}p)p^{e-2}}, \end{cases}$$

where $t_i \equiv \gamma^i \Delta / (p^{e-1} \text{tr}(\delta z_{i,0})) \pmod{p}$ and

$$k_{i,j} \equiv \left(\text{tr}(\gamma z_{i-1,j}) - \text{tr}(z_{i,0} u^{jt_i p^{e-2}}) \right) / (p^e \text{tr}(z_{i,0} \delta)) \pmod{p}.$$

For $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, p-1$,

$$\text{tr}(\gamma z_{i-1,j}) \equiv \text{tr}(\gamma z_{i-1,0} u^{jt_{i-1} p^{e-2}}) \equiv \text{tr}(z_{i,0}) + j \gamma^i \Delta p^{e-1} \equiv \text{tr}(z_{i,0} u^{jt_i p^{e-2}}) \pmod{p^e},$$

hence $\text{tr}(z_{i,j}) \equiv \text{tr}(\gamma z_{i-1,j}) \pmod{p^{e+1}}$, i.e. $(\text{tr}(z_{i-1,j}), \text{tr}(z_{i,j})) \in R_{e+1}^b(\alpha, \beta)$.

Denote $u_{i,j} = (z_{i,j}/z_{i,0} - 1)/p^{e-1}$. Notice that $u_{i,j} \equiv jt_i \delta \pmod{p}$ for $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, p-1$. By Lemma 3, $\text{tr}(z_{0,0} u_{0,j}) \equiv j \Delta / p^{e-1} \pmod{p}$.

Since for $i = 0, 1, \dots, m-1$,

$$\text{tr}(z_{i+1,j}) - \text{tr}(z_{i+1,0}) \equiv \text{tr}((z_{i,j} - z_{i,0})\gamma) \equiv \gamma_0(\text{tr}(z_{i,j}) - \text{tr}(z_{i,0})) + p^{\ell+e-1} \gamma_0 \text{tr}(\gamma_\ell z_{i,0} u_{i,j}) \pmod{p^{e+1}},$$

we have

$$\begin{aligned} & (\text{tr}(z_{m,j}) - \text{tr}(z_{0,j})) - (\text{tr}(z_{m,0}) - \text{tr}(z_{0,0})) \\ & \equiv (\text{tr}(z_{m,j}) - \text{tr}(z_{m,0})) - (\text{tr}(z_{0,j}) - \text{tr}(z_{0,0})) \\ & \equiv (\gamma_0^m - 1)(\text{tr}(z_{0,j}) - \text{tr}(z_{0,0})) + p^{\ell+e-1} \sum_{i=0}^{m-1} \gamma_0^{m-i} \text{tr}(\gamma_\ell z_{i,0} u_{i,j}) \pmod{p^{e+1}}, \end{aligned}$$

yielding

$$\begin{aligned} \Delta' & \equiv \sum_{j=0}^{p-1} \sum_{i=0}^{m-1} (\text{tr}(z_{i+1,j}) - \text{tr}(z_{i,j})) \\ & \equiv \sum_{j=0}^{p-1} (\text{tr}(z_{m,j}) - \text{tr}(z_{0,j})) \\ & \equiv p\Delta + (\gamma_0^m - 1)p^{e-1} \sum_{j=1}^{p-1} \text{tr}(z_{0,0} u_{0,j}) + p^{\ell+e-1} \sum_{i=0}^{m-1} \gamma_0^{m-i} \sum_{j=1}^{p-1} \text{tr}(z_{i,0} u_{i,j} \gamma_\ell) \pmod{p^{e+1}}. \end{aligned}$$

For $\ell \geq 2$, it is clear that $\Delta' \equiv p\Delta \pmod{p^{e+1}}$ and $v(\Delta') = e$. For $p \geq 3$,

$$\begin{aligned} \sum_{j=1}^{p-1} \text{tr}(z_{0,0}u_{0,j}) &\equiv \Delta p(p-1)/(2p^{e-1}) \equiv 0 \pmod{p}; \\ \sum_{j=1}^{p-1} \text{tr}(z_{i,0}u_{i,j}\gamma_\ell) &\equiv \text{tr}(z_{i,0}\delta\gamma_\ell)p(p-1)/2 \equiv 0 \pmod{p}. \end{aligned}$$

and recalling $\gamma_0^m - 1 \in p^\ell A_e$, we have $\Delta' \equiv p\Delta \pmod{p^{e+1}}$ and hence $v(\Delta') = e$.

Since $(\text{tr}(z_{i,j}), \text{tr}(z_{i+1,j})) \in R_{e+1}^b(\alpha, \beta)$ for $i = 0, 1, \dots, m-1$ and $j = 0, 1, \dots, p-1$, then by transitivity $(\text{tr}(z_{0,0}), \text{tr}(z_{m,p-1})) \in R_{e+1}^b(\alpha, \beta)$, i.e. $(a, a + \Delta') \in R_{e+1}^b(\alpha, \beta)$. By Lemma 3, $a + p^e \mathbb{Z}_p$ is bold in $R_{e+1}^b(\alpha, \beta)$. Furthermore, given that S is bold in $R_e^b(\alpha, \beta)$, by transitivity S is hence also bold in $R_{e+1}^b(\alpha, \beta)$. \square

Lemma 7. Assume $p \geq 3$ or $e = p = 2$, and let $1 \leq r(\gamma) \leq e$. If $\sigma(x)$ is primitive, then $\{z\gamma^i : i \in \mathbb{Z}\} + p^{r(\gamma)} A_e \in \mathcal{P}(R_e(\alpha, \beta))$ for any $z \in A_e^*$. If $\sigma(x)$ is strongly primitive, then $\mathcal{P}(R_e(\alpha, \beta)) = \mathcal{C}_\gamma$.

Proof. Let $\gamma = \gamma_0(1 + \gamma_\ell p^\ell)$, where $\ell = r(\gamma)$, i.e. $\gamma_0 \in \mathbb{Z}_p$ and $\gamma_\ell \in O^* \setminus \mathbb{Z}_p$.

Firstly, if $z \in \{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$ then

$$\{z\gamma^i \pmod{p^\ell} : i \in \mathbb{Z}\} \in \mathcal{P}(R_\ell(\alpha, \beta)). \quad (10)$$

Now consider $e = p = 2$ and $r(\gamma) = 1$. Without loss of generality, suppose $\gamma_0 = 1$. By Lemma 1, for any $a \in \{0, 1, 2, 3\}$, there exists w satisfying

$$\begin{cases} \text{tr}(w) &\equiv a \pmod{2}, \\ \text{tr}(w\gamma_1) &\equiv 1 \pmod{2}. \end{cases}$$

Thus $(a, a + 2) \in R_2(\alpha, \beta)$ for some $a \in \{0, 2\}$ and for some $a \in \{1, 3\}$, implying $\mathcal{P}(R_2(\alpha, \beta)) = \{\{0, 2\}, \{1, 3\}\}$.

Now consider $p \geq 3$. Given w satisfying

$$\begin{cases} \text{tr}(w) &\equiv a \pmod{p}, \\ \text{tr}(w\delta) &\not\equiv 0 \pmod{p}, \end{cases} \quad (11)$$

we have $(a, \gamma_0(a + p^\ell \text{tr}(w\gamma_\ell))) \in R_{\ell+1}^b(\alpha, \beta)$. Denote

$$D = \left\{ \overline{\text{tr}(w\gamma_\ell)} : \text{tr}(w) \equiv a \pmod{p}, w \in S_\alpha^b \right\}.$$

By Lemma 1, if $1, \bar{\delta}, \bar{\gamma}_\ell$ are \mathbb{F}_p -linear independent, then $D = \mathbb{F}_p$; otherwise, if $\bar{\gamma}_\ell = r_0 + r_1 \bar{\delta}$ then $D = \mathbb{F}_p \setminus \{r_0 \bar{a}\}$. Thus, by Lemma 3, for $t \in \{0, 1, \dots, p-1\}$, we have $(a + tp^\ell, \gamma_0 a + (j + t\gamma_0)p^\ell) \in R_{\ell+1}^b(\alpha, \beta)$ for $j \in \{0, 1, \dots, p-1\}$ at most except for $(a + tp^\ell, \gamma_0 a + (r_0 \bar{a} + t\gamma_0)p^\ell)$. Note $p \geq 3$ and then for any a and $j \in \mathbb{Z}/p\mathbb{Z}$, $(a, a\gamma_0^2 + jp^\ell) \in R_{\ell+1}^b(\alpha, \beta)^{(T)}$. Therefore, by transitivity the set $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_{\ell+1}$ is bold in $R_{\ell+1}(\alpha, \beta)$. By Lemma 6, $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_e$ is bold in

$R_e(\alpha, \beta)$. The set $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_e$ is included in an equivalence class of $R_{\ell+1}^b(\alpha, \beta)^{(E)}$, and it is an equivalence class by Fact 3 and Eq.(10).

If $\sigma(x)$ is primitive and $a \in \mathbb{Z}_p^*$, then Eq.(11) is solvable, and hence $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_e \in \mathcal{P}(R_e(\alpha, \beta))$. If $\sigma(x)$ is strongly primitive, then Eq.(11) is solvable for any $a \in \mathbb{Z}_p$, and hence $\mathcal{P}(R_e(\alpha, \beta)) = \{\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_e : a \in A_e\}$. \square

Condition 2. Assume $p = 2$ and

$$\left\{ \text{tr}(z) \pmod{4} : \overline{\text{tr}(u_1 z)} = 0, z/\alpha \in W \right\} = \{0, 1, 2, 3\}.$$

Lemma 8. Let $e > p = 2$ and $\ell = r(\gamma) \geq 2$. Assume $\gamma = \gamma_0(1 + 2^\ell \gamma_\ell)$, where $\gamma_0 \in \mathbb{Z}_2$. Suppose (i) $\overline{\gamma_\ell} \notin \{\overline{\delta}, 1 + \overline{\delta}\}$ and Condition 2 holds, or (ii) $\overline{\gamma_\ell} \notin \{1 + \overline{u_1}, 1 + \overline{u_1}^2, 1 + \overline{\delta}, \overline{u_1}, \overline{u_1}^2, \overline{\delta}\}$. If $\sigma(x)$ is primitive, then $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_e \in \mathcal{P}(R_e(\alpha, \beta))$ for $a \in \mathbb{Z}_2^*$; If $\sigma(x)$ is strongly primitive, then $\mathcal{P}(R_e(\alpha, \beta)) = \mathcal{C}_\gamma$.

Proof. Similar to the proof of Lemma 7, due to Lemma 6, it is sufficient to show that $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_{\ell+1}$ is bold in $R_{\ell+1}(\alpha, \beta)$ for any $a \in \{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$.

Choose any $a \in \{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$ and $b \in \mathbb{F}_2$.

If (ii) holds, i.e. $1, \overline{u_1}, \overline{\delta}, \overline{\gamma_\ell}$ are \mathbb{F}_2 -linear independent, then for both $b = 0$ and $b = 1$, there exists $w \in \mathbb{F}_q$ satisfying

$$\begin{cases} \text{tr}(w) & \equiv a \pmod{2}, \\ \text{tr}(wu_1) & \equiv 1 \pmod{2}, \\ \text{tr}(w\delta) & \equiv 1 \pmod{2}, \\ \text{tr}(w\gamma_\ell) & \equiv b \pmod{2}. \end{cases} \quad (12)$$

By Lemma 4, there exists $z \in S_\alpha^b$ such that $\text{tr}(z) \equiv a \pmod{p^{\ell+1}}$ and $\text{tr}(z\gamma) \equiv \gamma_0 \text{tr}(z) + p^\ell b \pmod{p^{\ell+1}}$. Thus, $(a, \gamma_0 a) \in R_{\ell+1}^b(\alpha, \beta)$ and $(a, \gamma_0 a + p^\ell) \in R_{\ell+1}^b(\alpha, \beta)$. By transitivity, $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_{\ell+1}$ is bold in $R_{\ell+1}(\alpha, \beta)$.

Now suppose that (i) holds. If Eq.(12) is solvable for both $b = 0$ and $b = 1$, the statement also holds. Otherwise, $\overline{\gamma_\ell} = r_0 + \overline{u_1} + r_2 \overline{\delta}$, where $r_0, r_2 \in \mathbb{F}_2$, and for some $b_0 \in \mathbb{F}_2$ Eq.(12) is solvable for $b = b_0$ but insolvable for $b = b_0 + 1 \in \{0, 1\}$. See $\text{tr}(w\gamma_\ell) \equiv r_0 a + 1 + r_2 = b_0 \pmod{2}$. Thanks to Condition 2, there exists $w \in \mathbb{F}_q$ satisfying

$$\begin{cases} \text{tr}(w) & \equiv a \pmod{4}, \\ \text{tr}(wu_1) & \equiv 0 \pmod{2}, \\ \text{tr}(w\delta) & \equiv 1 \pmod{2}, \\ \text{tr}(w\gamma_\ell) & \equiv b_0 + 1 \pmod{2}. \end{cases}$$

Since now $\text{tr}(w\gamma_\ell) \equiv r_0 a + 0 + r_2 = b_0 + 1 \pmod{2}$. By Lemma 4, there exists $z \in S_\alpha^b$ such that $\text{tr}(z) \equiv a \pmod{2^{\ell+1}}$ and $\text{tr}(z\gamma) \equiv \gamma_0 \text{tr}(z) + p^\ell(b_0 + 1) \pmod{p^{\ell+1}}$. Thus, $(a, \gamma_0 a) \in R_{\ell+1}^b(\alpha, \beta)$ and $(a, \gamma_0 a + 2^\ell) \in R_{\ell+1}^b(\alpha, \beta)$. By transitivity, $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_{\ell+1}$ is bold in $R_{\ell+1}(\alpha, \beta)$. \square

By Fact 1, Fact 2, Lemma 7, Lemma 8 and Theorem 4,

Theorem 6. Let $\vec{s}_\alpha, \vec{s}_\beta \in G_e(\eta)$ and $r(\gamma) \geq 1$. Assume (i) $p \geq 3$, or (ii) $p = e = 2$, or (iii) $e \geq r(\gamma) \geq p = 2$ and $\overline{\gamma}_\ell \notin \{1 + \overline{u}_1, 1 + \overline{u}_1^2, 1 + \overline{\delta}, \overline{u}_1, \overline{u}_1^2, \overline{\delta}\}$, or (iv) $e \geq r(\gamma) \geq p = 2$ and $\overline{\gamma}_\ell \notin \{\overline{\delta}, 1 + \overline{\delta}\}$ and Condition 2 holds. If $\sigma(x)$ is primitive and $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$ then ψ is constant on $\{a\gamma^i : i \in \mathbb{Z}\} + p^\ell A_e$ for any $a \in A_e^*$; if $\sigma(x)$ is strongly primitive, then $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$ if and only if ψ admits \mathcal{C}_γ .

Below is an example wherein $\mathcal{P}(R_e(\alpha, \beta))$ is not so regular as \mathcal{C}_γ .

Example 3. Take $p = 2$ and $e = 4$. Let w be a root of $x^4 + x + 1$. Choose $\eta = -7w^3 - 6w^2 - 7w - 1$, $\alpha = 1$ and $\beta = -4w^2 + 8w - 7$. See $r(\gamma) = 2$ and $\overline{\gamma}_2 = 1 + \overline{\delta}$. Computation shows that

$$\mathcal{P}(R_4(\alpha, \beta)) = \{\{-1, 3, -5\}, \{7\}, \{1, -3, 5, -7\}, \{0, \pm 4, 8\}, \{\pm 2, \pm 6\}\}.$$

Remark 6. When $\sigma(x)$ is strongly primitive, till now in our experiment of toy examples $\mathcal{P}(R_e(\alpha, \beta)) \neq \mathcal{C}_\gamma$ occurs only if $\overline{\gamma}_\ell = 1 + \overline{\delta}$, even if $\ell = 1$; and it is desirable to decide whether $\mathcal{P}(R_e(\alpha, \beta)) = \mathcal{C}_\gamma$ for $\overline{\gamma}_\ell \in \{1 + \overline{u}_1, 1 + \overline{u}_1^2, \overline{u}_1, \overline{u}_1^2, \overline{\delta}\}$.

Proof of Theorem 1. If $r(\gamma) < e$, then Statements (i) and (ii) hold by Theorem 5 and Theorem 6.

Now suppose $r(\gamma) = e$, i.e. $\gamma \in A_e$. For $e = p = 2$, $\gamma = -1$ and hence ψ is constant on $\{\pm 1\}$. For $p \geq 3$, if $\gamma^{p-1} \not\equiv 1 \pmod{p^e}$, then $1 + p^{e-1} \in \{\gamma^i : i \in \mathbb{Z}\}$ because the multiplicative group A_e^* is isomorphic to the additive group $\mathbb{Z}/(p-1)\mathbb{Z} \times A_{e-1}$. Thus, ψ is constant on $\{a + ip^{e-1} : i = 0, 1, \dots, p-1\}$ for $a \in \{\vec{s}_\alpha(i) : i \in \mathbb{Z}\}$. Statements (i) and (ii) also hold. The rest is $\gamma^m = 1$, where $1 < m \mid (p-1)$. Clearly, m can be chosen to be prime. \square

Proof of Theorem 2. Since $\sigma(x)$ is primitive and $\overline{\delta}^2 \notin \mathbb{F}_p$, $\sigma(x)$ is actually strongly primitive. Following from Theorem 5, Theorem 6 and Theorem 1, $\widehat{\psi}$ is not injective on $G_e(\eta)$ if and only if there exist $0 \leq \ell \leq e$ and an m -th root of unity γ such that ψ is constant on $\{\gamma^i a : i \in \mathbb{Z}\} + p^\ell A_e$ for any $a \in A_e$. \square

4 Some explicit compressing maps

In this section we give new entropy-preserving maps from A_e to \mathbb{F}_p for $p \geq 3$.

In this section any $a \in A_e$ is identified as its unique representative in $\{0, 1, \dots, p^e - 1\}$, and $a_i \in \mathbb{F}_p$ is defined by $a = a_0 + pa_1 + \dots + a_{e-1}p^{e-1}$, where $a_i \in \{0, 1, \dots, p-1\}$. In the literature [7, 8, 15, 16, 23, 24, 26, 30, 34, 35], without ambiguity a is identified with the vector $(a_0, a_1, \dots, a_{e-1}) \in \mathbb{F}_p^e$ and thereby a map on A_e is explicitly written as an e -variable function on \mathbb{F}_p . Conventionally, each function from \mathbb{F}_p^e to \mathbb{F}_p is written as a multivariate polynomial in which the degree in each variable is less than p .

Firstly, we give another proof of entropy preservation of the modular compression [35].

Theorem 7 (Zhu-Qi). Let p be an odd prime, M a positive integer not a power of p , and a map $\psi(x) = x \pmod{M}$ defined on A_e . If $\sigma(x)$ is primitive, then $\widehat{\psi}$ is injective on $G_e(\eta)$.

Proof. See that M is not a power of p . Hence, for any $a \in A_e$ we have $\psi(a + jp^{e-1}) \neq \psi(a + (j+1)p^{e-1})$ for some $j \in \{0, 1, \dots, p-1\}$. Thus, neither Statement (i) nor (ii) of Theorem 1 holds.

Suppose $1 < \gamma < p^e$ and $\gamma^m \equiv 1 \pmod{p^e}$ for some $1 < m \mid p-1$. If $M \nmid \gamma-1$, then $\psi(\gamma) \neq \psi(1)$. Consider $M \mid \gamma-1$. There exists $a \in A_e^*$ satisfying $a \equiv 1/(\gamma-1) \pmod{p^e}$. Clearly, $a < p^e-1$. Hence, $a\gamma = a+1$ and we have $\psi(a\gamma) \neq \psi(a)$. Thus, Statement (iii) of Theorem 1 does not hold, either.

By Theorem 1, $\widehat{\psi}$ is injective on $G_e(\eta)$. \square

If $\sigma(x)$ is not strongly primitive, polynomials like (4) do not necessarily induce injective maps on $G_e(\eta)$. Below is an example.

Example 4. Use the notations in Example 1. Let $\beta = 12w+13$ and $\alpha = -\beta$. The map $\psi : A_e \rightarrow \mathbb{F}_p$ is defined as $\psi(x) = x_{e-1}^2 + x_{e-1}$. Then $\widehat{\psi}(\vec{s}_\alpha) = \widehat{\psi}(\vec{s}_\beta)$.

In the following two theorems, we give three families of functions from A_e to \mathbb{F}_p which induce injective maps on $G_e(\eta)$.

Theorem 8. Let p be an odd prime and let $\sigma(x)$ be strongly primitive. The map $\psi : A_e \rightarrow \mathbb{F}_p$ is defined by

$$\psi(x) = f_0(x_{e-1})f_1(x_0, x_1, \dots, x_{e-2}) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $f_0 \in \mathbb{F}_p[x_{e-1}]$ and $f_1, f_2 \in \mathbb{F}_p[x_0, x_1, \dots, x_{e-2}]$. If $1 \leq \deg f_0 < p$, $(x_0^{p-1} - 1) \nmid f_1$ and $f_1(0, 0, \dots, 0) \neq 0$, then the induced map $\widehat{\psi}$ is injective on $G_e(\eta)$.

Proof. Without ambiguity we denote $f_j(x) = f_j(x_0, x_1, \dots, x_{e-2})$ for $x \in A_e$, $j = 1, 2$. See $f_j(x + ip^{e-1}) = f_j(x)$ for any $i \in \mathbb{F}_p$.

Since $(x_0 - i) \nmid f_1$ for some $i \in \mathbb{F}_p^*$, there exists $a \in A_e^*$ satisfying $f_1(a) \neq 0$, and hence ψ is not constant on $a + p^{e-1}A_e$. Additionally, $f_1(0) \neq 0$ and ψ is not constant on $p^{e-1}A_e$. Thus, neither Statement (i) nor (ii) of Theorem 1 holds.

Now suppose for some $\gamma \in A_e$, $\psi(\gamma a) = \psi(a)$ for any $a \in A_e$, where $m = \min \{i : \gamma^i \equiv 1 \pmod{p^e}\}$ and $1 < m \mid p-1$. For $1 \leq i < e$ and $x \in A_e$, denote by $[x]_i$ the integer satisfying $[x]_i \equiv x \pmod{p^i}$ and $0 \leq [x]_i < p^i$; $\{x\}_i = (\gamma[x]_i - [\gamma x]_i)/p^i \pmod{p}$. Particularly, $\{x\}_0 = 0$. Clearly, $\{a\}_i = \{a + jp^i\}_i$ for any $j \in \mathbb{F}_p$.

Claim. If $a \neq 0$, then there exists $k \in \{1, 2, \dots, m\}$ satisfying $\{a\gamma^k\}_i \neq 0$. Otherwise, suppose $\{\gamma^j a\}_i = 0$ for any $j \in \{1, 2, \dots, m\}$, then $(\gamma^j a)_i = \{\gamma^{j-1} a\}_i + \overline{\gamma}(\gamma^{j-1} a)_i = \overline{\gamma}^j a_i$. Since $1 \leq [\gamma^j a]_i < p^i$, we have $m \leq \sum_{i=1}^m [\gamma^j a]_i < mp^i$ and hence $p^{i+1} \nmid \sum_{i=1}^m [\gamma^j a]_i$. However, seeing $\gamma^j a \equiv [\gamma^j a]_i + p^i(\gamma^j a)_i \pmod{p^{i+1}}$, we have

$$\sum_{j=1}^m [\gamma^j a]_i \equiv \sum_{j=1}^m [\gamma^j a]_i + p^i a_i \sum_{j=1}^m \overline{\gamma}^j \equiv \sum_{j=1}^m [\gamma^j a]_i + p^i \sum_{j=1}^m (\gamma^j a)_i \equiv \sum_{j=1}^m \gamma^j a \equiv 0 \pmod{p^{i+1}},$$

which is absurd.

Notice $\psi(p^{e-1}x_{e-1}) = f_0(x_{e-1})f_1(0) + f_2(0)$. Because $\psi(p^{e-1}x_{e-1}\gamma) = \psi(p^{e-1}x_{e-1})$ and $f_1(0) \neq 0$, we have $f_0(x_{e-1}) = f_0(\overline{\gamma}x_{e-1})$, i.e., $f_0(x_{e-1}) = g(x_{e-1}^m)$, where $g \in \mathbb{F}_p[x_{e-1}]$ and $1 \leq \deg g < p/m$. By the assumption $\psi(\gamma x) = \psi(x)$, we have for any $\Delta \in \mathbb{F}_p$, $\psi(x + p^{e-1}\Delta) - \psi(x) = \psi(\gamma x + p^{e-1}\gamma\Delta) - \psi(\gamma x)$, implying

$$(g((\Delta + \{x\}_{e-1}/\overline{\gamma})^m) - f_0((\gamma x)_{e-1})) f_1(\gamma x) = (g(\Delta^m) - f_0(x_{e-1})) f_1(x). \quad (13)$$

As above, there exists $a \in A_e^*$ with $f_1(a) \neq 0$. If $f_1(\gamma^i a) \neq f_1(\gamma^{i-1} a)$ for some $i \in \{1, 2, \dots, m\}$, then the terms in Δ of the highest degree do not coincide in Eq.(13) for $x = \gamma^{k-1} a$, where $k = \min \{1 \leq i \leq m : f_1(\gamma^i a) \neq f_1(a)\}$. Hence, suppose $f_1(\gamma^i a) = f_1(a)$ for any $i \in \{1, 2, \dots, m\}$. As claimed above, there exists $b \in \{\gamma^i a : i = 1, 2, \dots, m\}$ with $\{b\}_{e-1} \neq 0$. Now letting $x = b$, the terms in Δ of the second highest degree do not coincide in Eq.(13). Thus, the assumption is absurd and Statement (iii) of Theorem 1 does not hold.

By Theorem 1, $\widehat{\psi}$ is injective on $G_e(\eta)$. □

Remark 7. The polynomial (4) is a special case of Theorem 8, and hence Theorem 8 improves [24, 30, 34].

Theorem 9. Let p be an odd prime and let $\sigma(x)$ be primitive. The map $\psi : A_e \rightarrow \mathbb{F}_p$ is defined by

$$\psi(x) = x_{e-1}^\ell f_1(x_0, x_1, \dots, x_{e-2}) + f_2(x_0, x_1, \dots, x_{e-2}),$$

where $1 \leq \ell < p$ and $f_1, f_2 \in \mathbb{F}_p[x_0, x_1, \dots, x_{e-2}]$. If (i) $\ell = 1$, $f_1 = g_0(x_k) + g_1(x_0, x_1, \dots, x_{k-1})$, $\gcd(p-1, \deg g_0 + 1) = 1$, $1 \leq \deg g_0 < p$ if $1 \leq k \leq e-2$ and $x_0 \nmid g_0$ if $k = 0$; or (ii) $2 \leq \ell < p$, $(x_0^{p-1} - 1) \nmid f_1$ and $x_0 \nmid f_1$; then the induced map $\widehat{\psi}$ is injective on $G_e(\eta)$.

Proof. Use the same notations as in the proof of Theorem 8.

Similarly, as $(x_0^{p-1} - 1) \nmid f_1$ and $x_0 \nmid f_1$, there exists $a \in A_e^*$ and $b \in pA_e$ satisfying $f_1(a)f_1(b) \neq 0$, and hence ψ is constant neither on $a + p^{e-1}A_e$ nor on $b + p^{e-1}A_e$. Thus, neither Statement (i) nor (ii) of Theorem 1 holds.

Now suppose for some $\gamma \in A_e$, $\psi(\gamma a) = \psi(a)$ for any $a \in A_e^*$, where $m = \min \{i : \gamma^i \equiv 1 \pmod{p^e}\}$ and $1 < m \mid p-1$. Then for any $\Delta \in \mathbb{F}_p$, $\psi(x + p^{e-1}\Delta) - \psi(x) = \psi(\gamma x + p^{e-1}\gamma\Delta) - \psi(\gamma x)$, i.e.,

$$f_1(x)(\Delta^\ell - x_{e-1}^\ell) = f_1(\gamma x)((\gamma\Delta + \{x\}_{e-1})^\ell - (\gamma x)_{e-1}^\ell).$$

Comparing terms in Δ of the (second) highest degree, we have $f_1(x) = \overline{\gamma}^\ell f_1(\gamma x)$ and $\{x\}_{e-1} f_1(\gamma x) = 0$ if $\ell \geq 2$; $f_1(x) = \overline{\gamma} f_1(\gamma x)$ if $\ell = 1$. As claimed in the proof of Theorem 8, for any $a \in A_e^*$, there exists $i \in \{1, 2, \dots, m\}$ satisfying $\{\gamma^i a\}_{e-1} \neq 0$. If $\ell \geq 2$, taking $x = \gamma^i a$, we have $f_1(a) = \overline{\gamma}^{\ell(i+1)} f_1(\gamma^{i+1} a) = 0$, contradictory to $(x_0^{p-1} - 1) \mid f_1$. If $\ell = 1$, for any $x \in A_e^*$ and any $\Delta \in \mathbb{F}_p$, $f_1(x + p^k \Delta) - f_1(x) = \overline{\gamma}(f_1(\gamma(x + p^k \Delta)) - f_1(\gamma x))$. Comparing the term in Δ of the highest degree, we conclude $m \mid (\deg g_0 + 1)$. If $\gcd(p-1, \deg g_0 + 1) = 1$, then $m \nmid (\deg g_0 + 1)$ since $m \mid (p-1)$. Therefore, Statement (iii) of Theorem 1 does not hold.

By Theorem 1, under given conditions $\widehat{\psi}$ is injective on $G_e(\eta)$. □

Remark 8. The polynomials (2) and (3) are special cases of Theorem 9, and then Theorem 9 improves [23, 30].

5 Conclusion

We study the inherent information of a compressing map which acts on distinct primitive sequences generated by the same LFSR over $\mathbb{Z}/p^e\mathbb{Z}$. For an odd prime, a clear criterion of entropy preservation is given if $(x^{(q-1)} - 1)^2 / p^2 \not\equiv a \pmod{(p, \sigma(x))}$ for any $a \in \mathbb{F}_p$. Furthermore, we also

present three new kinds of entropy-preserving maps. Finally, it is of interest to consider the following two problems: (i) What is $\mathcal{P}(R_e(\alpha, \beta))$ if $\sigma(x)$ is strongly primitive and $(x^{(q-1)} - 1)^2/p^2 \equiv a \pmod{(p, \sigma(x))}$ for some $a \in \mathbb{F}_p$? Does it hold that $\mathcal{P}(R_e(\alpha, \beta)) = \{A_e\}$ if $\sigma(x)$ is of large degree and $\overline{\gamma} \notin \mathbb{F}_p$? (ii) What is exactly $\mathcal{P}(R_e(\alpha, \beta))$ if $p = 2$, $\alpha \equiv \beta \pmod{2}$ and $\sigma(x)$ is strongly primitive?

References

- [1] H.-J. Chen, W.-F. Qi: On the distinctness of maximal length sequences over $Z/(pq)$ modulo 2, *Finite Fields Appl.*, vol.15, no.1, pp.23–39 (2009)
- [2] Z. D. Dai: Binary sequences derived from ML-sequences over rings I: Periods and minimal polynomials, *J. Crypt.*, vol.5, no.4, pp.193–207 (1992)
- [3] Z. D. Dai, T. Beth, D. Gollman: Lower bounds for the linear complexity of sequences over residue ring, in *Advances in Cryptology-EUROCRYPT’90*, Berlin, Germany:Springer, 1991, LNCS 473, pp.189–195.
- [4] S.-Q. Fan, W.-B. Han: Random properties of the highest level sequences of primitive sequences over \mathbf{Z}_{2^e} , *IEEE Transactions on Information Theory*, vol.49, no.6, 1553–1557, June (2003)
- [5] J. Gallier, *Discrete mathematics*, Springer, New York (2011)
- [6] H.-G. Hu, D.-G. Feng, W.-L. Wu: Incomplete exponential sums over galois rings with applications to some binary sequences derived from Z_{2^t} , *IEEE Transactions on Information Theory*, vol.52, no.5, 2260–2265, May (2006)
- [7] M.-Q. Huang: Analysis and cryptologic evaluation of primitive sequences over an integer residue ring, Ph.D. dissertation, Graduate School of USTC, Academia Sinica, Beijing, China (1988) (in Chinese)
- [8] M.-Q. Huang, Z.-D. Dai: Projective maps of linear recurring sequences with maximal p -adic periods, *Fibonacci Quart.*, vol.30, no.2, pp.139–143, (1992)
- [9] A. S. Kuzmin: Lower estimates for the ranks of coordinate sequences of linear recurrent sequences over primary residue rings of integers, *Russian Math. Surv.*, vol.48, no.3, pp.203–204 (1993)
- [10] A. S. Kuzmin, V. L. Kurakin, A. V. Mikhalev, A. A. Nechaev: Linear recurring sequences over rings and modules, *J. Math. Sci.*, vol.76, no.6, pp.2793–2915 (1995)
- [11] A. S. Kuzmin, A. A. Nechaev: Linear recurring sequences over Galois rings, *Algebra Logic*, vol.34, no.2, pp.87–100 (1995)
- [12] A. S. Kuzmin, A. A. Nechaev: Linear recurring sequences over Galois ring, *Russian Math. Surv.*, vol.48, no.1, pp.171–172 (1993)
- [13] R. Lidl, H. Niederreiter: Finite fields, in *Encyclopedia of Mathematics and its Applications*, Addison-Wesley Publishing Company, Inc. U.S.A. (1983)

- [14] A. A. Nechaev: Linear recurring sequences over commutative rings, *Discrete Math.*, vol.3, no.4, pp.107–121 (1991)
- [15] W.-F. Qi: Compressing maps of primitive sequences over $\mathbb{Z}/(2^e)$ and analysis of their derivative sequences, Higher Education Press, Beijing (2001) (in Chinese)
- [16] W.-F. Qi, J.-H. Yang, J.-J. Zhou: ML-sequences over rings $\mathbb{Z}/(2^e)$, in *Advances in Cryptology—ASIACRYPT’98*, Berlin, Germany: Springer-Verlag, 1998, LNCS 1514, pp.315–326.
- [17] W.-F. Qi, J.-J. Zhou: The distribution of 0 and 1 in the highest level sequence of primitive sequences over $\mathbb{Z}/(2^e)$, *Sci. China, ser.A*, vol.27, no.4, pp.311–316 (1997) (in Chinese)
- [18] W.-F. Qi, J.-J. Zhou: The distribution of 0 and 1 in the highest level sequence of primitive sequences over $\mathbb{Z}/(2^e)$ (II), *Chinese Sci. Bull.*, vol.42, no.18, pp.1938–1940 (1997) (in Chinese)
- [19] W.-F. Qi, X.-Y. Zhu: Compressing mappings on primitive sequences over $\mathbb{Z}/(2^e)$ and its Galois extension, *Finite Fields Appl.*, vol.8, pp.570–588, (2002)
- [20] A. M. Robert: *A course in p -adic analysis*, Springer, New York, (2000)
- [21] J.-P. Serre: *A course in arithmetic*, Springer, New York (1973)
- [22] P. Solé, D. Zinoviev: The most significant bit of maximum-length sequences over \mathbb{Z}_{2^l} : autocorrelation and imbalance, *IEEE Transactions on Information Theory*, vol.50, no.8, 1844–1846, August (2004)
- [23] Z.-H. Sun, W.-F. Qi: Injective maps on primitive sequences over $\mathbb{Z}/(p^e)$, *Appl. Math. J. Chinese Univ. Ser.B*, 22(4):469–477 (2007)
- [24] T. Tian, W.-F. Qi: Injectivity of compressing maps on primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Transactions on Information Theory*, vol.53, no.8, 2960–2966, August (2007)
- [25] M. Ward: The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.*, vol.35, pp.600–628, July (1933)
- [26] K.-C. Zeng, Z.-D. Dai, M.-Q. Huang: Injectiveness of mappings from ring sequences to their sequences of significant bits, *Symposium on Problems of Cryptology*, State Key Laboratory of Information Security, Beijing, China, 1995, pp.132–141.
- [27] Q.-X. Zheng, W.-F. Qi: Distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Transactions on Information Theory*, vol.56, no.1, 555–563, January (2010)
- [28] Q.-X. Zheng, W.-F. Qi: A new result on the distinctness of primitive sequences over $\mathbb{Z}/(qp)$ modulo 2, *Finite Fields Appl.*, vol.17, no.3, pp.254–274 (2011)
- [29] Q.-X. Zheng, W.-F. Qi, T. Tian: On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers, *IACR Cryptology ePrint Archive*, 2012:3 (2012)
- [30] X.-Y. Zhu, W.-F. Qi: Compression mappings on primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Transactions on Information Theory*, vol.50, no.10, pp.2442–2448, October (2004)

- [31] X.-Y. Zhu, W.-F. Qi: Uniqueness of the distribution of zeros of primitive level sequences over $\mathbb{Z}/(p^e)$, *Finite Fields Appl.*, vol.11, pp.30–44, (2005)
- [32] X.-Y. Zhu, W.-F. Qi: The nonlinear complexity of level sequences over $\mathbb{Z}/(4)$ *Finite Fields Appl.*, vol.12, pp.103–127, (2006)
- [33] X.-Y. Zhu, W.-F. Qi: Uniqueness of the distribution of zeros of primitive level sequences over $\mathbb{Z}/(p^e)$ (II), *Finite Fields Appl.*, vol.13, pp.230–248, (2007)
- [34] X.-Y. Zhu, W.-F. Qi: Further result of compressing maps on primitive sequences modulo odd prime powers, *IEEE Transactions on Information Theory*, vol.53, no.8, 2985–2990, August (2007)
- [35] X.-Y. Zhu, W.-F. Qi: On the distinctness of modular reductions of maximal length sequences modulo odd prime powers, *Mathematics of Computation*, 77(263):1623–1637, July (2008)